AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, James V. Richardson, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and am assigned to the office of the Resident Agent in Charge, Providence, RI. I have been an agent of HSI since 2009. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, and the transfer of obscene material to minors, including but not limited to, violations of 18 U.S.C. §§ 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. I am currently participating in an investigation relating to violations of federal law by Raymond GLIOTTONE for possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). I submit this affidavit in support of an application to search a OnePlus Nord N100 cell phone (hereinafter "SUBJECT PROPERTY") owned by Raymond GLIOTTONE (hereinafter "GLIOTTONE"), which was seized by the United States Probation Office (USPO) on or about April 15, 2021, and the content of the SUBJECT PROPERTY or media located therein, as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.

3. The statements contained in this affidavit are based in part on my own investigation; information provided by the United States Probation Office; and my experience, training, and background as a Special Agent with HSI. Because this affidavit is being submitted for the limited purpose of securing authorization for requested search warrant, I have not included every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

4. In April 2021, I was contacted by the United States Attorney's Office regarding an individual, Raymond GLIOTTONE (DOB XX/XX/1983), who I previously investigated and arrested in 2018. In that investigation, GLIOTTONE was communicating with a minor female and planning to travel to the state of Maine to pick the minor female up and engage in illicit sexual acts. GLIOTTONE also exchanged sexually explicit images with the minor female.

5. On November 16, 2018, HSI Providence agents, assisted by the Rhode Island State Police (RISP)/Internet Crimes Against Children (ICAC) Task Force, executed a federal search warrant, issued by this court, at GLIOTTONE's residence in Cranston, RI. GLIOTTONE admitted to communicating with the minor female, having sexually explicit conversations with the minor female, and exchanging sexually explicit images with the minor female. GLIOTTONE claimed he did not know the female was a minor at the time she sent him sexually explicit images, but acknowledged that he kept the images even after learning she was a minor. GLIOTTONE was subsequently arrested and charged with possession and access with intent to view child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) and coercion and enticement of a minor in violation of 18 U.S.C. § 2422(b).

6. In February 2019, GLIOTTONE pleaded guilty to an Information charging him with attempted interstate travel for the purpose of engaging in any sexual act with a minor in violation of 18 U.S.C. § 2423(B). In March 2019, GLIOTTONE was sentenced to 24 months of incarceration followed by 10 years of supervised release. GLIOTTONE was released from federal custody on September 18, 2020.

7. On April 16, 2021, I was contacted by the United States Attorney's Office (USAO) in Providence, RI regarding a possible violation of GLIOTTONE's supervised release. According to the information received from the United States Probation Office (USPO) through the USAO, GLIOTTONE was observed by the USPO using an unapproved smart phone while on break at his place of employment. GLIOTTONE was approached by the USPO and the smart phone was seized by the USPO. The USPO conducted a cursory check of GLIOTTONE's smart phone and discovered that GLIOTTONE was using the chat application Kik and was paying for images and videos. The USPO stated that they saw some nude images of "young" girls. GLIOTTONE was interviewed by the USPO and admitted to receiving approximately 20 images from a 13-year-old, paying for 7 of the images. GLIOTTONE claimed he did not know the girl was 13 at the time he received the images.

8. The day after seizing GLIOTTONE's smart phone, the USPO was contacted by GLIOTTONE's manager at his place of employment. According to GLIOTTONE's manager, GLIOTTONE stated that there were "bad pics" on the seized phone and that he was trying to figure out a way to do a remote factory reset of the smart phone, which could have the effect of erasing any data from the phone.

9. On May 4, 2021, I took custody of GLIOTTONE's OnePlus Nord N100 cell phone and placed it in the HSI evidence room.

CHARACTERISTICS COMMON TO PERSONS WHO ENGAGE IN

CHILD SEXUAL EXPLOITATION

10. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have collaborated, I have learned that there are certain characteristics that are generally common to offenders who access, send, distribute, exhibit, possess, display, transport, manufacture, or produce material which depicts minors engaged in sexually explicit conduct, or who engage in sexually explicit communications with minors. Said material includes, but is not limited to, photographs and videos stored electronically on computers, digital devices, or related digital storage media.

11. Such offenders may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have that stem from viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in photographs or other visual media, or from literature describing such activity.

12. Such offenders may collect sexually explicit or suggestive materials in a variety of media, including digital photographs, videos, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to facilitate contact offenses – that is, to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

13. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a, "SD card," computer or surrounding area, or on their phones. These child pornography images are often maintained for several years and are kept close by, usually at the offender's residence, inside the offender's vehicle, or, at times, on his person, to enable the individual to view the child

pornography images, which are highly valued.[1]

14. Some of these individuals, however, have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, presumably to avoid criminal liability. Importantly, as described in more detail below, evidence of such activity, including deleted child pornography, often can be located on these individuals' smartphones, computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[2]

15. Such offenders also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists or other record of individuals with whom they have been in contact and who share the same interests in child pornography. Often times such correspondence takes the form of "chats," "groups" or direct or private messages within social media applications. Such offenders prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

16. Based upon the foregoing, I believe that Raymond GLIOTTONE likely displays characteristics common to individuals who access with the intent to view and possess, collect, receive, or distribute child pornography. As such, I submit that there is probable cause to believe

[1] *See United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections);

[2] *See United States v. Seiver*, 692 F.3d 774, 775-776 (7th Cir. 2012) (in context of staleness challenge, collecting and agreeing with cases from the 4th, 5th, 6th, and 9th Circuits that acknowledge the ability of forensic examiners to recover evidence of child pornography even after such files are deleted by a user).

that contraband material depicting minors engaged in sexually explicit conduct and other evidence, instrumentalities, and fruits of violations of possession and access with intent to view child pornography 18 U.S.C. §§ 2252(a)(4) exist on the SUBJECT PROPERTY.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

17. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

18. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media ("computer equipment") be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

a. The volume of evidence: Storage media such as smart phones can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements: Analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system

and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

CONCLUSION

19. Based on the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), as described in Attachment B, are located within the SUBJECT PROPERTY, as more fully described in Attachment A.

JAMES V. RICHARDSON
Special Agent, Department of Homeland Security

JAMES V. RICHARDSON
Special Agent
Homeland Security Investigations

Attested to be the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Telephone.** *(specify reliable electronic means)*

Date	*Judge's signature*
City and State	*Printed name and title*

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

The property to be searched include:

A. One (1) OnePlus Nord N100 cell phone, model #BE2015.

ATTACHMENT B
DESCRIPTION OF INFORMATION TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), including:

A. Records and tangible objects pertaining to the following topics:

1. Child pornography and child erotica;

2. Obscene materials;

3. Communications with minors or others having access to minors that relate to the persuasion, inducement, enticement or coercion of a minor to engage in sexual activity for which any person could be charged with a criminal offense, or the transfer of obscene materials to a minor, or the distribution or receipt of child pornography.

4. Evidence of who used, owned, or controlled the computer equipment;

5. Evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

6. Evidence of the attachment of other computer hardware or storage media;

7. Evidence of counter forensic programs and associated data that are designed to eliminate data;

8. Evidence of the times the computer equipment was used;

9. Passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

10. Pecords and tangible objects pertaining to accounts held with companies

providing Internet access or remote storage of either data or storage media; and

11. Evidence indicating the computer user's state of mind as it relates to the crime under investigation.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, gaming device, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or

transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

H. “Obscene material” is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.